Przemysław Alkowski[1]

Bezpieczeństwo informacyjne – zarys wybranych aspektów w kontekście problemu bezpieczeństwa państwa

1. Uwagi wstępne

Współczesne oblicze bezpieczeństwa jest zagadnieniem bardzo szerokim, obejmującym swoim zasięgiem różne sfery życia. Jest to szczególnie widoczne, gdy na tematykę bezpieczeństwa patrzy się przez pryzmat kryterium przedmiotowego. Pozwala ono dokonać podziału, według którego można wyróżnić bezpieczeństwo militarne, polityczne, ekonomiczne, społeczne czy wreszcie informacyjne. To ostatnie zasługuje na szczególną uwagę, ze względu na swój unikatowy charakter. Bezpieczeństwo informacyjne może stanowić przedmiot rozważań sam w sobie, jednak jak dokona się dokładniejszej analizy, można stwierdzić, że często stanowi zasadniczą metodę oddziaływania, a przynajmniej wpływa na wymienione powyżej rodzaje bezpieczeństwa.

Samo bezpieczeństwo informacyjne nie jest zagadnieniem nowym, jego ślady pojawiły „się już w VI w. p.n.e. dzięki chińskiemu filozofowi Sun Tzu, który (...) opracował pierwsze strategie walki informacyjnej, mającej na celu osiągnięcie zwycięstwa nad przeciwnikiem bez walki"[2]. Jednak szczególnego wydźwięku nabrało w ostatnich kilkudziesięciu latach (od ok. lat 60. XX wieku), kiedy to nasiliły się procesy globalizacji, digitalizacji, a społeczeństwo można było określać mianem informacyjnego.

Opracowanie to ma na celu zarysowanie następujących kwestii: czym jest informacja (a w konsekwencji bezpieczeństwo informacyjne), jaka jest istota walki informacyjnej i jak ona się odbywa, jakie są sposoby pozyskiwania informacji i cel, jakiemu mają one służyć. Finalnie, jaki jest skutek pozyskania informacji oraz jak prezentuje się system bezpieczeństwa informacyjnego Rzeczypospolitej Polskiej (w oparciu z jednej strony o działalność określonych organów państwa, z dru-

1 Uniwersytet w Białymstoku.

2 M. Plecka, A. Rychły-Lipińska, *Bezpieczeństwo informacyjne*, [w:] A. Urbanek (red.), *Wybrane problemy bezpieczeństwa*, Słupsk 2013, s. 163.

giej natomiast o podstawowe akty prawne – warunkujące istnienie systemu i jego sprawne funkcjonowanie).

2. Pojęcie informacji i bezpieczeństwa informacyjnego

Aby dokładnie zobrazować obrany temat, należy wyjść od ustalenia, czym w ogóle jest informacja, by móc mówić o bezpieczeństwie informacyjnym. Pozornie się wydaje, iż nie powinno to stanowić większego problemu. Większość osób „czuje", czym informacja jest, jednak przybranie tego w ramy kilkuzdaniowej definicji stwarza już trudności. Nie jest to zadanie proste, gdyż każdemu procesowi poznawczemu człowieka towarzyszy proces uzyskiwania, posiadania oraz przetwarzania informacji. Efektem tych czynności jest osiągnięcie określonego stanu – wiedzy, która to jest oceniana pod kątem treści, źródła jej pochodzenia, potencjalnej możliwości wykorzystania, uwzględniając walory praktyczno-teoretyczne[3]. Dlatego też informacja to dobro (intelektualne) o charakterze niematerialnym. W tym kontekście ważnym elementem definicyjnym jest stopień wartości informacji pozwalający określić poziom możliwego wykorzystania, przydatności. Ostatecznie decyduje on o rodzaju podejmowanych decyzji. Wartość informacyjna jest poddawana gradacji, gdzie każdej treści można przypisać odpowiednio wydźwięk dodatni, zerowy lub ujemny. Przy czym dodatni pozwala efektywniej zwiększyć prawdopodobieństwo osiągnięcia założonego celu, natomiast wynik ujemny cel ten oddala[4].

Po tak poczynionych ustaleniach można podjąć próbę określenia, czym jest bezpieczeństwo informacyjne. Poprzednia definicja, na samym wstępie, pozwala ustalić, iż bezpieczeństwo informacyjne jest pojęciem szerokim, możliwym do ujęcia z różnych perspektyw. Implikuje to mnogość możliwości definiowania. Najbardziej elastycznym opisem jest stwierdzenie, że „bezpieczeństwo informacyjne stanowi zbiór działań, metod, procedur, podejmowanych przez uprawnione podmioty, zmierzające do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych poprzez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją czy zniszczeniem"[5].

Podobny charakter przybiera definicja, według której „bezpieczeństwo informacyjne dotyczy zagwarantowania sobie przez dany podmiot (np. państwo) integralności, kompletności, wiarygodności posiadanych zasobów informacyjnych w każdej formie, nie tylko informatycznej. Odnosi się więc zarówno do wszelkiego rodzaju wysiłków, służących ochronie posiadanych informacji istotnych w kontekście bezpieczeństwa (a więc mających wpływ na funkcjonowanie struktur państwo-

3 A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem informacyjnym*, Warszawa 2010, s. 10-20.
4 M. Plecka, A. Rychły-Lipińska, op. cit., s. 169-170.
5 P. Potejko, *Bezpieczeństwo informacyjne*, [w:] K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), *Bezpieczeństwo państwa*, Warszawa 2009, s. 194.

wych i społeczeństwa), jak i zapewnieniu przewagi informacyjnej przez zdobywanie nowych lub bardziej aktualnych danych oraz akcje dezinformacyjne wobec ewentualnych przeciwników (państw lub innych podmiotów)"[6]. Można również charakteryzować bezpieczeństwo informacyjne w oparciu o atrybuty bezpieczeństwa informacji[7]. Wśród nich wymienia się takie jak: poufność, autentyczność, dostępność, integralność danych, integralność systemu, integralność, rozliczalność i niezawodność.

Tabela 1. Definicje atrybutów bezpieczeństwa danych i informacji

Nazwa atrybutu bezpieczeństwa	Definicja
Integralność (*integrity*)	Zapewnienie, że dane lub informacje nie zostały zmienione w sposób nieautoryzowany (dokładne i kompletne aktywa).
Poufność (*confidentiality*)	Dane i informacje udostępniane są tylko osobom upoważnionym.
Dostępność (*availability*)	Możliwość wykorzystania na każde żądanie w założonym czasie przez upoważnione podmioty.
Niezawodność (*reliability*)	Oznacza koherentne, zamierzone zachowanie i skutki.
Autentyczność (*authenticity*)	Zapewnienie, że tożsamość podmiotu lub zasobu jest zgodna z deklarowaną.
Rozliczalność (*accountability*)	Pewność, że działania danego podmiotu są w sposób jednoznaczny przypisane temu podmiotowi.
Niezaprzeczalność (*non-repudiation*)	Brak możliwości wyparcia się swego uczestnictwa w przetwarzaniu danych.

Źródło: G. Ożarek, Normalizacyjne aspekty bezpieczeństwa informacyjnego, Referat został wygłoszony w dniu 17 września 2010 r. na sympozjum naukowym – „Metrologia w systemach zarządzania", 15-17 września, Dymaczewo k/Poznania, zorganizowanym przez Polskie Forum ISO[8].

Jednakże definicja ta (jakkolwiek przydatna) prowadzi do nieuprawnionego zawężenia do zakresu pojęcia bezpieczeństwa teleinformatycznego – stanowiącego część składową bezpieczeństwa informacyjnego. W literaturze przedmiotu wśród określeń można spotkać ponadto wyróżnienie pewnych elementów, takich jak: dostępność wykorzystywania informacji dla uprawnionych osób[9], warunki wewnętrz-

6 M. Madej, *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009, s. 18.

7 Idąc za A. Białasem, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Warszawa 2006, s. 34.

8 http://www.pkn.pl/sw-publikacje (20.09.2014).

9 M. Plecka, A. Rychły-Lipińska, op. cit., s. 165.

no-zewnętrzne pozwalające na funkcjonowanie społeczeństwa informacyjnego[10] również w kontekście ochrony informacji niejawnych.

Uogólniając (chcąc przybliżyć istotę), pod hasłem „bezpieczeństwo informacyjne" nie kryje się nic innego jak stan, gdy jeden podmiot (w tym wypadku państwo) może (i czyni to) gromadzić, posiadać, a w razie potrzeby wykorzystać różnego rodzaju dane (będące swoistego gatunku informacją) do osiągnięcia określonego przez niego celu. Musi to się jednak odbywać w sprzężeniu z bezpieczeństwem, odpornością na ingerencję innych podmiotów, które to znowuż mają interes w wejściu w posiadanie takich danych. Dopiero taka definicja, mająca charakter negatywno-pozytywny, w sposób pełny buduje obraz bezpieczeństwa informacyjnego.

3. Walka informacyjna

W obecnej dobie rozwoju cywilizacyjnego, gdy następuje intensywna informatyzacja różnych dziedzin życia społecznego (a w konsekwencji też państwowego), informacja nabiera szczególnego znaczenia. Umiejętne się nią posługiwanie może wpłynąć na funkcjonowanie państwa, różnych jego dziedzin. Właśnie to „umiejętne posługiwanie" staje się przedmiotem walki. Jej uczestnikami są zarówno podmiot gromadzący określone informacje, jak i przeciwnik tego pierwszego podmiotu, którego zadaniem jest albo ingerowanie, albo przynajmniej kontrola znajomości treści gromadzonej informacji. Świadczy to o tym, że musi nastąpić „kooperacja negatywnie wzajemna, przynajmniej dwupodmiotowa, realizowana w sferach: zdobywania informacji, zakłócenia informacyjnego i obrony informacyjnej, gdzie każdemu działaniu jednej strony przyporządkowane jest działanie antagonistyczne strony drugiej"[11].

W polskiej nauce spotkać się można z definicją, iż walkę informacyjną stanowi zorganizowana „w formę przemocy aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływających przez nie informacji oraz ochronę własnych systemów informacyjnych przed podobnym działaniem przeciwnika"[12].

W różnych państwach definiowanie tego pojęcia jest niekiedy odmienne. Jednak jego sens sprowadza się do tego samego. Istotnym elementem jest występowanie specyficznego celu prowadzonych przez poszczególne państwa działań. Jest nim uzyskanie przewagi strategiczno-taktycznej, zmierzającej do obezwładnienia prze-

10 E. Nowak, M. Nowak, *Zarys teorii bezpieczeństwa narodowego*, Warszawa 2011, s. 103.
11 L. Ciborowski, *Walka informacyjna*, Toruń 1999, s. 187.
12 T. Jemioło, P. Sienkiewicz (red.), *Zagrożenia dla bezpieczeństwa informacyjnego państwa (Identyfikacja, analiza zagrożeń i ryzyka)*, t. 1, *Raport z badań*, Warszawa 2004, s. 74.

ciwnika, co następnie pozwala wywalczyć i utrzymać przewagę nad przeciwnikiem w dziedzinie informacyjnej[13].

Metody działania państw mogą przybierać bardzo różnorodne postacie. Ich spektrum będzie zależne od wielu czynników, poczynając od pomysłowości zleceniodawców, kończąc na warunkach polityczno-społecznych. Może to się odbywać poprzez wprowadzanie do systemów informatycznych, tzw. złośliwego oprogramowania, jakim są wirusy komputerowe zdolne do szybkiego samopowielania się. Również instalowanie „bomb logicznych", pozwalających się uaktywnić na zdalnie nadany sygnał. W końcu wysyłanie impulsów o wysokiej mocy, które są zorientowane na niszczenie sprzętu elektronicznego[14]. Działania te mają bardzo doniosły wymiar, szczególnie w czasie ogólnokrajowej cyfryzacji, digitalizacji i informatyzacji wszystkich sfer życia, w tym także działalności państwa. Bez względu na to, jakie metody by to nie były, ich ocena zawsze odbywa się przez pryzmat efektywności. Dlatego też nie można zapominać o konwencjonalnych sposobach działań, czego znowu przykładem może być działalność szpiegowska.

Agenci – szpiedzy mogliby wydawać się rozwiązaniem przestarzałym, jednak jest to mylne wyobrażenie, szczególnie w obliczu ostatnich sensacyjnych doniesień o wykryciu przez polskie Służby Kontrwywiadu Wojskowego, a następnie zatrzymaniu przez Agencję Bezpieczeństwa Wewnętrznego i Żandarmerię Wojskową dwóch osób podejrzanych o szpiegostwo na rzecz obcego państwa (Rosji). Zestawiając to z funkcją wysoko postawionych urzędników państwowych, przez których to przechodziły istotne ze strategicznego punktu informacje w zakresie energetyki i obronności, i w obliczu trwających działań wojennych na wschodzie Ukrainy, w oczywisty sposób dochodzi się do konkluzji, że walka informacyjna trwa stale i odbywa się różnymi metodami. Ilość natomiast pozyskanych albo przynajmniej zniekształconych informacji pozwoli na określenie siły, potencjału danego podmiotu (państwa).

Istotny jest też fakt, iż o ile słowo „walka" może nasuwać skojarzenia okołomilitarne, to błędem by było utożsamianie tego wyłącznie z tą sferą. Jej zakres jest szerszy i wykazuje cechy o charakterze pozamilitarnym[15]. Odbywająca się walka ma miejsce zarówno w trakcie wojny, ale też różnego rodzaju kryzysów czy nawet w czasie pokoju[16]. Jej zadaniem jest stworzenie stanu, kiedy szeroko rozumiany przeciwnik będzie miał utrudnioną możliwość poznania faktycznego stanu rzeczy-

13 A. Żebrowski, *Bezpieczeństwo informacyjne Polski a walka informacyjna*, „Rocznik Kolegium Analiz Ekonomicznych" 2013, nr 29, s. 454.

14 L. Ciborowski, *Potencjalne zagrożenia – identyfikacja i charakterystyka*, „Myśl Wojskowa" 2000, nr 4, s. 86-87.

15 A. Żebrowski, *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej. (Wywiad i kontrwywiad w latach 1989-2003)*, Kraków 2005, s. 30.

16 A. Żebrowski, *Bezpieczeństwo informacyjne*..., op. cit., s. 455.

wistości. Niemożliwość poznania prawdy o osobach, zdarzeniach, zjawiskach wpływać ma na podejmowanie właściwych decyzji[17].

Specyficzną rolę, ale również bardzo istotną, przy tworzeniu i rozpowszechnianiu informacji odgrywają media. Ich misja uaktualnia się właśnie w kontekście sfery pozamilitarnej, gdyż proces zdobywania informacji rozszerzył się na informacje nie tylko o charakterze niejawnym[18]. Zauważa się to na szczeblu państwowym – w sektorze publicznym, choć też coraz częściej w sektorze prywatnym. Obszary walki wkraczają w takie sfery jak sytuacja wojskowa, polityczna, społeczna, ale także naukowa i gospodarcza (gdzie największym zainteresowaniem cieszy się szeroko rozumiany sektor paliwowo-energetyczny). Udział mediów, będących bezpośrednim uczestnikiem procesu informacyjnego, stał się pewnego rodzaju *novum* jakościowym. Realizują one określone role w wymiarze zarówno podstawowym (dostarczając wiadomości o aktualnym stanie państwa), jak i pozapodstawowym.

Sygnalizowana nowość polega na wprowadzaniu do obiegu dużej ilości nowych, niepotwierdzonych, nierzadko mało wartościowych a zarazem trudno sprawdzalnych informacji[19]. Przekazywanie ich w postaci ukierunkowanych komentarzy doskonale wpisuje się w schemat walki. Tworzy to swoistego rodzaju chaos informacyjny, co w oczywisty sposób wpływa na percepcję określonych podmiotów, poddanych silnym procesom propagandowym i manipulacyjnym. Co ciekawe, opisane działania są efektem świadomie realizowanych założeń oraz bardzo często przypadkowych, niezamierzonych tzw. lapsusów językowych (szczególnie popularnych w środowisku politycznym).

4. System bezpieczeństwa informacyjnego

Mówiąc o systemie bezpieczeństwa informacyjnego, można stwierdzić, iż odbywa się dwupłaszczyznowo. Z jednej strony realizuje się poprzez działalność określonych organów państwa, które w zakresie swoich kompetencji mają za zadanie ochronę państwa przed planowanymi działaniami mogącymi godzić w niepodległość państwa, w jego stabilność wewnętrzną, w funkcjonowanie struktur państwowych, przez co mogą naruszać szeroko rozumiane interesy państwa. Wśród takich służb należy wymienić Agencję Bezpieczeństwa Wewnętrznego (która została powołana w celu ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego)[20], Agencję Wywiadu (w sprawach ochrony bezpieczeństwa

17 A. Żebrowski, M. Żmigrodzka, *Media uczestnikami walki informacyjnej*, „Doctrina. Studia Społeczno-Polityczne" 2012, nr 9, s. 359.

18 Ibidem.

19 Ibidem.

20 Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2010 r. Nr 29, poz. 154), art. 1.

zewnętrznego państwa)[21], Służbę Wywiadu Wojskowego (właściwą w sprawach ochrony przed zagrożeniami zewnętrznymi dla obronności państwa, bezpieczeństwa i zdolności bojowej)[22] oraz Służbę Kontrwywiadu Wojskowego (właściwą w sprawach ochrony przed zagrożeniami wewnętrznymi dla obronności państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych Rzeczypospolitej Polskiej)[23].

Z drugiej strony ustawodawca przewidział określone instytucje prawne, które określają, jakie informacje mogą i powinny być upubliczniane oraz jakie takiego waloru powinny być i są pozbawione. Do zasadniczych aktów normatywnych regulujących, mających wpływ na stan istnienia i funkcjonowania systemu bezpieczeństwa informacyjnego, należy zaliczyć Konstytucję Rzeczypospolitej Polskiej[24], ustawę o dostępie do informacji publicznej[25], ustawę o ochronie danych osobowych[26], ustawę o dostępie do informacji niejawnej[27], a także kodeks karny[28].

Konstytucja jako tzw. ustawa zasadnicza reguluje zakres obowiązków i uprawnień, jakie przysługują każdemu obywatelowi. Również znajdują się w niej zapisy w zakresie pozyskiwania informacji. Konstytucja, w art. 54, gwarantuje wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji. Jest to swoistego rodzaju „odpowiedź" na realizację zasady demokratycznego państwa prawa a zarazem dbałość o przejrzystość i uczciwość życia społecznego.

Jeszcze dobitniej jest to realizowane poprzez art. 61, gdzie obywatelowi przyznaje się prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Dotyczy to również uzyskiwania informacji o działalności organów samorządu gospodarczego i zawodowego, a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim realizują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa.

Ponadto uzyskiwanie informacji dotyczy też dostępu obywatela do dokumentów, jak i możliwości wstępu na posiedzenia kolegialnych organów władzy – nawet z możliwością rejestracji dźwięku lub obrazu. Oba te prawa są na tyle istotne, że ich ograniczenie może nastąpić wyłącznie w wypadku, gdy wpłynąć mogą na ochronę wolności i praw innych osób bądź podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa.

Ustawa o dostępie do informacji publicznej określa zasady i tryb udostępniania i ponownego wykorzystania informacji o sprawach publicznych, stanowiących in-

21 Ibidem, art. 2.
22 Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. z 2014 r., poz. 253), art. 2.
23 Ibidem, art. 1.
24 Konstytucja Rzeczypospolitej Polskiej z dnia 4 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483).
25 Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2014 r., poz. 782).
26 Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r., poz. 1182).
27 Ustawa z dnia 5 stycznia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r. Nr 182, poz. 1228).
28 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. z 1997 r. Nr 88, poz. 553 ze zm.).

formację publiczną. Określa podmioty (zarówno te publiczne, jak i inne) zobowiązane do udostępnienia informacji publicznej. Ponadto akt ten wymienia, na czym polegają uprawnienia realizujące prawo dostępu. Istotną kwestią jest też wyliczenie, jakie kwestie mogą ograniczać dostęp. Traktuje o tym art. 5, gdzie wymieniono, iż tyczy się to ochrony informacji niejawnych oraz ochrony innych tajemnic ustawowo chronionych, prywatności osoby fizycznej lub tajemnicy przedsiębiorcy (o ile osoby te nie zrezygnują z przysługujących im praw).

W system ochrony bezpieczeństwa informacyjnego wpisuje się też ustawa o ochronie danych osobowych, która pozwala przetwarzać dane osobowe, określając przy tym zasady właściwego postępowania i prawa osób fizycznych. Podkreśla się, że musi się to odbywać w poszanowaniu dobra publicznego, dobra osoby, której dane dotyczą, lub dóbr osób trzecich w zakresie i trybie określonych ustawą.

Bardzo istotnym aktem prawnym traktującym o bezpieczeństwie informacyjnym jest ustawa o ochronie informacji niejawnych. Ustawa ta określa, czym jest informacja niejawna, a dodatkowo zawiera zasady ochrony tych informacji. Uznaje ona, iż nieuprawnione ujawnienie może spowodować lub powoduje szkody dla Rzeczypospolitej Polskiej albo ujawnienie to byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie opracowywania informacji oraz niezależnie od formy i sposobu ich wyrażania.

Do takich zasad należą: klasyfikowanie informacji niejawnych; organizowanie ochrony informacji niejawnych; przetwarzanie informacji niejawnych; postępowanie sprawdzające prowadzone w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy, zwanego dalej odpowiednio „postępowaniem sprawdzającym" lub „kontrolnym postępowaniem sprawdzającym"; postępowanie prowadzone w celu ustalenia, czy przedsiębiorca nim objęty zapewnia warunki do ochrony informacji niejawnych, zwanego dalej „postępowaniem bezpieczeństwa przemysłowego"; organizacja kontroli stanu zabezpieczenia informacji niejawnych; ochrona informacji niejawnych w systemach teleinformatycznych; stosowanie środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych.

Ustawę stosuje się do Sejmu i Senatu, Prezydenta Rzeczypospolitej Polskiej, organów administracji rządowej, organów jednostek samorządu terytorialnego, a także innych podległych im jednostek organizacyjnych lub przez nie nadzorowanych, sądów i trybunałów, organów kontroli państwowej i ochrony prawa (jako do organów władzy publicznej); do jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych; do Narodowego Banku Polskiego; do państwowych osób prawnych i innych państwowych jednostek organizacyjnych; do jednostek organizacyjnych podległych organom władzy publicznej lub nadzorowanych przez te organy; do przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umów związanych z dostępem do informacji nie-

jawnych lub wykonujących takie umowy albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych.

Ustawa dokonuje specyfikacji informacji niejawnych ze względu na wystąpienie: wyjątkowo poważnej szkody, poważnej szkody oraz samej szkody. Uwzględniając powyższy czynnik klasyfikujący, wyróżnia się informacje o klauzuli odpowiednio:

a) ściśle tajne (powodujące wyjątkowo poważną szkodę przez zagrożenie niepodległości, suwerenności i integralności terytorialnej RP, zagrożenie bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu RP, zagrożenie pozycji międzynarodowej RP, zagrożenie sojuszom, osłabienie gotowości obronnej RP, doprowadzenie do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie, zagrożenie życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie, zagrożenie życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych),

b) tajne (powodujące poważną szkodę przez uniemożliwienie realizacji zadań związanych z ochroną suwerenności lub porządku konstytucyjnego RP, pogorszenie stosunków RP z innymi państwami lub organizacjami międzynarodowymi, zakłócenie przygotowania obronnego państwa lub funkcjonowania Sił Zbrojnych RP, utrudnienie wykonywania czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione, zakłócenie w istotny sposób funkcjonowania organów ścigania i wymiaru sprawiedliwości, przyniesienie strat znacznych rozmiarów w interesach ekonomicznych RP),

c) poufne (powodujące szkodę przez utrudnienie prowadzenia bieżącej polityki zagranicznej RP, utrudnienie realizacji przedsięwzięć obronnych lub negatywne wpływanie na zdolność bojową Sił Zbrojnych RP, zakłócenie porządku publicznego lub zagrożenie bezpieczeństwu obywateli, utrudnienie wykonywania zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów RP, utrudnienie wykonywania zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości, zagrożenie stabilności systemu finansowego RP, wpływanie niekorzystnie na funkcjonowanie gospodarki narodowej).

Dodatkowo, jeżeli nie nadano informacjom wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych RP, wówczas nadaje się im klauzulę „zastrzeżone".

Omawiana ustawa przewiduje system ochrony informacji niejawnych, którego funkcjonowanie jest nadzorowane przez przytaczane wcześniej służby – Agencję Bezpieczeństwa Wewnętrznego oraz Służbę Kontrwywiadu Wojskowego. W zakresie ich kompetencji leży zgodnie z art. 10 ust. 1 prowadzenie kontroli ochrony informacji niejawnych i przestrzeganie obowiązujących przepisów w tym zakresie, realizowanie zadań w zakresie bezpieczeństwa systemów teleinformatycznych, prowadzenie postępowań sprawdzających oraz kontrolnych postępowań sprawdzających, a także postępowań bezpieczeństwa przemysłowego, zapewnienie ochrony informacjom niejawnym wymienianym między RP a innymi organizacjami międzynarodowymi lub państwami, prowadzenie szkoleń i doradztwa w zakresie ochrony informacji niejawnych.

Postępowania sprawdzające pozwalają określić, czy sprawdzana osoba daje rękojmię zachowania tajemnicy. Natomiast w jego toku sprawdza się, czy wystąpiły: uczestnictwo, współpraca lub popieranie przez sprawdzaną osobę działalności szpiegowskiej, sabotażowej, terrorystycznej albo innej ukierunkowanej przeciwko RP, uzasadnione zagrożenie werbunku lub nawiązania kontaktu z osobą sprawdzaną przez służby specjalne obcego wywiadu, przestrzeganie po stronie sprawdzanego porządku konstytucyjnego RP – uwzględniając w szczególności udział w funkcjonowaniu organizacji bądź partii politycznych o charakterze totalitarnym bądź nastawionych rasistowsko, ukrywanie lub świadome niezgodne z prawdą podawanie w ankiecie bezpieczeństwa osobowego lub postępowaniu sprawdzającym przez osobę sprawdzaną informacji mających znaczenie dla ochrony informacji niejawnych, wystąpienie związanych z osobą sprawdzaną okoliczności powodujących ryzyko jej podatności na szantaż lub wywieranie presji, niewłaściwe postępowanie z informacjami niejawnymi (w zakresie doprowadzenia bezpośrednio do ujawnienia tych informacji osobom nieuprawnionym; będące efektem celowego działania; stwarzające realne zagrożenie ich nieuprawnionym ujawnieniem, a nie miało to charakteru incydentalnego; finalnie ustalenie, czy nie dopuściła się tego osoba szczególnie zobowiązana na podstawie ustawy do ochrony informacji niejawnych: pełnomocnik ochrony, jego zastępca lub kierownik kancelarii tajnej).

Wątpliwości mogące wystąpić w toku prowadzenia postępowania sprawdzającego mogą dotyczyć: poziomu życia sprawdzanej osoby wyraźnie przewyższającego uzyskiwane przez nią dochody; informacji o chorobach psychicznych lub innych zakłóceniach czynności psychicznych mogących ograniczyć sprawność umysłową

oraz negatywnie wpływać na zdolność osoby sprawdzanej do wykonywania prac, związanych z dostępem do informacji niejawnych; uzależnienia od alkoholu, środków odurzających lub substancji psychotropowych.

Postępowanie sprawdzające kontrolne odbywa się w przypadku, gdy o osobie, której wydano poświadczenie bezpieczeństwa, zostaną ujawnione nowe informacje wskazujące, że nie daje ona rękojmi zachowania tajemnicy. W celu ich weryfikacji, przeprowadza się niezbędne czynności sprawdzające. Czynności te muszą być rzetelnie udokumentowane i prowadzone zgodnie z zasadami bezstronności, obiektywizmu i wykazania najwyższej staranności.

Ochronie informacji niejawnych w ramach bezpieczeństwa przemysłowego poświęcony jest rozdział IX omawianej ustawy. Przedsiębiorca sprawdzany jest pod kątem: struktury kapitału oraz powiązań kapitałowych przedsiębiorcy, źródeł pochodzenia środków finansowych i sytuacji finansowej; struktury organizacyjnej; systemu ochrony informacji niejawnych, w tym środków bezpieczeństwa fizycznego; kontroli wszystkich osób wchodzących w skład organów zarządzających, kontrolnych oraz osób działających z ich upoważnienia; natomiast w szczególnie uzasadnionych przypadkach kontrola osób posiadających poświadczenia bezpieczeństwa.

Do grona aktów prawnych regulujących kwestie bezpieczeństwa informacyjnego obowiązkowo należy zaliczyć również polski kodeks karny. Reguluje on odpowiedzialność karną za współpracę z obcym wywiadem oraz w rozdziale XXXIII traktuje o przestępstwach przeciwko ochronie informacji.

Artykuł 130 kk. stanowi, iż osoba, która bierze udział w działalności obcego wywiadu przeciwko Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności od roku do lat 10. W przypadku osób biorących udział w obcym wywiadzie albo działających na jego rzecz, udzielających temu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, przewiduje karę pozbawienia wolności na czas nie krótszy niż 3 lata. Jeśli natomiast ten, kto w celu udzielenia obcemu wywiadowi wymienionych wcześniej wiadomości gromadzi je lub przechowuje, wchodzi do systemu informatycznego w celu ich uzyskania albo zgłasza gotowość działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej, wtedy podlega karze pozbawienia wolności od 6 miesięcy do lat 8. Finalnie penalizowane jest organizowanie lub kierowanie działalnością obcego wywiadu, za co przewidziana jest kara pozbawienia wolności na czas nie krótszy od lat 5 albo karze 25 lat pozbawienia wolności.

Artykuły 265 i 266 kk. są swoistego rodzaju odpowiedzią wprost na zapisy w ustawie o ochronie informacji niejawnych. Pierwszy z nich przewiduje podleganie karze pozbawienia wolności od 3 miesięcy do lat 5 za ujawnienie lub wbrew przepisom ustawy wykorzystanie informacji niejawnych o klauzuli „tajne" lub „ściśle tajne". Jeśli taką informację ujawniono osobie działającej w imieniu lub na rzecz podmiotu zagranicznego, sprawca podlega wtedy karze pozbawienia wolności od

6 miesięcy do lat 8. W typie uprzywilejowanym łagodniej traktuje się osobę, która nieumyślnie ujawnia informacje o takich klauzulach, z którymi zapoznała się w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem. Wtedy podlega ona grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. W art. 266 kk., dotyczącym tajemnicy służbowej, jest mowa o odpowiedzialności osoby, która wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznała się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową. W takim wypadku podlega ona grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2, przy czym przestępstwo takie jest ścigane dopiero w następstwie złożenia wniosku przez pokrzywdzonego. Jeżeli funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli „zastrzeżone" lub „poufne" lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3.

Następne 6 artykułów tego rozdziału dotyczy kolejno odpowiedzialności karnej za: nielegalne uzyskanie informacji, niszczenie informacji, wyrządzenie szkody w bazach danych informatycznych, dokonanie sabotażu komputerowego, zakłócanie pracy w sieciach teleinformatycznych, a wreszcie za bezprawne wykorzystanie programów i danych.

5. Podsumowanie

Jak udało się w niniejszej pracy udowodnić, zagadnienie bezpieczeństwa informacyjnego nie jest zagadnieniem nowym, jednak w przeciągu ostatniego półwiecza zaktualizowało się i przybrało nowy wymiar. Szczególnie ten nowy wymiar jest dostrzegalny w kontekście nieustającej walki informacyjnej. Społeczeństwo jest jej stałym świadkiem, do czego wydatnie przyczynia się działalność mediów. Dostrzega się, iż w dojrzałych, ale przede wszystkim skutecznych kręgach kulturowych akt zbrojny to ostateczność. Odchodzi się od tych pierwotnych metod działania (gdzie narzędziem była oręż) na korzyść nowoczesnych, wywierających wpływ na psychikę ludzką. Taką właśnie metodę stanowi walka informacyjna.

Przytoczone szerokie znaczenie pojęć podstawowych (tj. informacji, bezpieczeństwa informacyjnego, walki informacyjnej) miało za zadanie wykazanie ich szerokiego zakresu znaczeniowego, a w konsekwencji też zarysowanie problemu owego bezpieczeństwa informacyjnego. Celem było pokazanie, jak zróżnicowane (pod względem charakteru) informacje mogą być przedmiotem rozważań w ramach bezpieczeństwa informacyjnego. Informacje te mogą w różny sposób mieścić się w ramach pojęcia danych osobowych czy też wprost informacji niejawnych. Dlatego właściwe uświadomienie sobie, jak szeroki zakres znaczeniowy mają powyższe

pojęcia, pozwoli należycie zadbać o właściwe funkcjonowanie systemu bezpieczeństwa informacyjnego państwa.

Literatura

Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Warszawa 2006.

Ciborowski L., *Potencjalne zagrożenia – identyfikacja i charakterystyka*, „Myśl Wojskowa" 2000, nr 4.

Ciborowski L., Walka informacyjna, Toruń 1999.

Jemioło T., Sienkiewicz P. (red.), *Zagrożenia dla bezpieczeństwa informacyjnego państwa (Identyfikacja, analiza zagrożeń i ryzyka)*, t. 1, *Raport z badań*, Warszawa 2004.

Madej M., *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [w:] M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009.

Nowak A., Scheffs W., *Zarządzanie bezpieczeństwem informacyjnym*, Warszawa 2010.

Plecka M., Rychły-Lipińska A., *Bezpieczeństwo informacyjne*, [w:] A. Urbanek (red.), *Wybrane problemy bezpieczeństwa*, Słupsk 2013.

Potejko P., *Bezpieczeństwo informacyjne*, [w:] K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), *Bezpieczeństwo państwa*, Warszawa 2009.

Żebrowski A., *Bezpieczeństwo informacyjne Polski a walka informacyjna*, „Rocznik Kolegium Analiz Ekonomicznych" 2013, nr 29.

Żebrowski A., *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej. (Wywiad i kontrwywiad w latach 1989-2003)*, Kraków 2005.

Żebrowski A., Żmigrodzka M., *Media uczestnikami walki informacyjnej*, „Doctrina. Studia Społeczno-Polityczne" 2012, nr 9.

Źródła prawa

Konstytucja Rzeczypospolitej Polskiej z dnia 4 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. z 1997 r. Nr 88, poz. 553 ze zm.).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r., poz. 1182).

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2010 r. Nr 29, poz. 154).

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2014 r., poz. 782).

Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. z 2014 r., poz. 253).

Ustawa z dnia 5 stycznia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r. Nr 182, poz. 1228).

Źródła internetowe

http://www.pkn.pl/sw-publikacje